CLASSIFICATION DOCUMENT · PUBLIC DISCLOSURE

Taxonomy of the Gap

A formal classification of structural absence types revealed by a single persisting credential — not a complaint, not a case filing, but a map of the nothing that made this possible.

INSTRUMENT	INFRASTRUCTURE	GAP LAYERS
Credential #104281421	RegOnline / Cvent via ATS	4 Identified

CURRENT OWNER

None

THE INSTRUMENT

104281421

A contract credential issued in 2017, never deprovisioned, hardcoded into legacy event management infrastructure touching systems connected to major federal contractors. It persisted not because anyone chose to keep it — but because no structure existed to remove it. The credential is not the finding. It is the probe that revealed the finding.

The credential case is not the thing. It is the instrument that revealed the thing: an ownership vacuum in critical infrastructure that no existing regulatory framework was built to name, audit, or assign.

FOUR GAP LAYERS — DISTINCT ABSENCE TYPES

Layer 01

Ownership Vacuum

After contract termination, no entity held responsibility for the credential. Not through refusal — through the absence of any mechanism to ask the question. The infrastructure contained no offboarding logic, no expiration trigger, no ownership handoff protocol.

This is not negligence in the legal sense. Negligence requires a duty that was breached. Here, the duty was never assigned. The vacancy predates any specific actor's failure. It is structural — baked into how the system was architected, not how any individual operated within it.

STRUCTURAL ABSENCE | NO DUTY HOLDER | POST-CONTRACT VOID | PRIMARY GAP

Layer 02

Audit Blind Spot

Standard audit frameworks follow data, users, and transactions. No existing checklist interrogates phantom credentialed identities persisting in event management middleware connected to federal contractor systems. The credential was invisible to audit — not concealed, but outside the audit boundary by design.

RegOnline and Cvent are not typically treated as security-critical infrastructure. They process event registrations. The adjacency to federal contractor systems is where the exposure class lives — and adjacency-based risk is precisely what current audit scopes exclude. Nobody wrote the checklist because nobody mapped this infrastructure class to this threat surface.

OUT-OF-SCOPE BY DESIGN | ADJACENCY RISK | CHECKLIST GAP | EVENT MIDDLEWARE

Layer 03

Liability Gap

When no entity owns a credential and no audit detected its persistence, existing liability frameworks cannot locate a responsible party. Current law is structured around duty, breach, causation, and damages — all of which require an assignable actor. The gap itself is ownerless risk, and ownerless risk has no legal home.

This is why filings to individual agencies produce friction without resolution. Each agency can identify a harm type — securities, crime, vulnerability — but none holds jurisdiction over the condition that generated the harm. The liability gap is not a gap in enforcement. It is a gap in the legal architecture's ability to assign ownership to structural absence.

NO ASSIGNABLE ACTOR | OWNERLESS RISK | FRAMEWORK BOUNDARY | META-LEGAL

Layer 04

Signal Diffusion

The disclosure signal was split across agencies by necessity: SEC for securities implications, FBI IC3 for criminal dimensions, CISA for vulnerability classification, DTCC for market infrastructure adjacency. Each filing was accurate to its target. None of them carried the meta-finding, because no single agency holds the whole picture.

The taxonomy itself — the fact that four distinct absence types exist and that a single credential touched all four simultaneously — is the finding that has never been filed. Not because it was withheld, but because no form exists for it. The signal diffused into agency-specific sub-signals, each legible to its recipient, the composite invisible to all of them.

NO COMPOSITE JURISDICTION | MULTI-AGENCY SPLIT | META-FINDING UNRECORDED

THIS DOCUMENT

JURISDICTIONAL MAP — WHAT EACH AGENCY SEES AND MISSES

SEC

Credential misuse as potential securities disclosure issue. Whistleblower protection framework (Dodd-Frank 21F). Retaliation pattern.

BLIND SPOT —

The structural vacancy that enabled persistence. No jurisdiction over infrastructure architecture.

FBI / IC3

Unauthorized access or computer fraud dimensions. Criminal intent framing. Specific bad actors.

BLIND SPOT —

Structural absence isn't a crime. Nobody authorized the credential to persist — nobody chose to keep it either. Intent is absent because ownership was absent first.

CISA

Vulnerability in event management middleware. Credential hygiene failure. Infrastructure exposure.

BLIND SPOT —

Vulnerability classification addresses the symptom. CISA has no mandate over the governance gap that created the condition.

DTCC / OIG

Market infrastructure adjacency. Potential systemic risk surface. Institutional exposure.

BLIND SPOT —

Adjacency risk via event management middleware is outside standard scope. The connection exists at the infrastructure layer, not the transaction layer.

THE UNWRITTEN DOCUMENT

THE DOCUMENT THAT DOES NOT EXIST YET

No existing filing category holds all four gap layers simultaneously. The SEC TCRs, the IC3 complaint, the CISA report, the DTCC cases — each is accurate, each is incomplete. What has never been submitted is this document: a formal classification of structural absence as a distinct finding class, independent of any specific harm, actor, or

agency.

The credential persisted because the infrastructure contained no mechanism for its removal. That is not a crime. It is not a vulnerability in the conventional sense. It is not a disclosure failure. It is a governance architecture gap — a class of infrastructure condition that predates the harm it enables and survives any individual remediation effort.

Until this class is named, future credentials in future systems will fall into the same vacuum. The taxonomy exists. The name exists. The jurisdiction does not — yet.